Task#1:

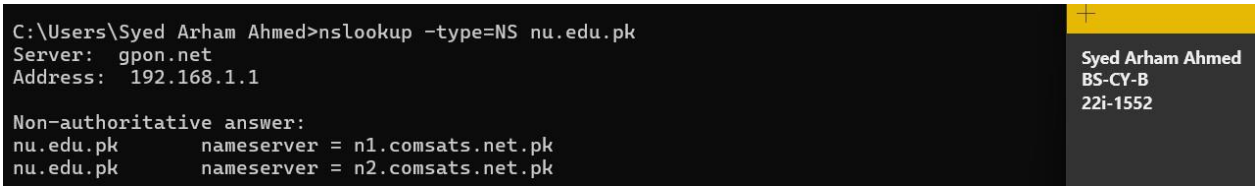
Q.1.

The IP for nu.edu.pk is 203.124.44.78 as shown in the screenshot above.

Q.2.

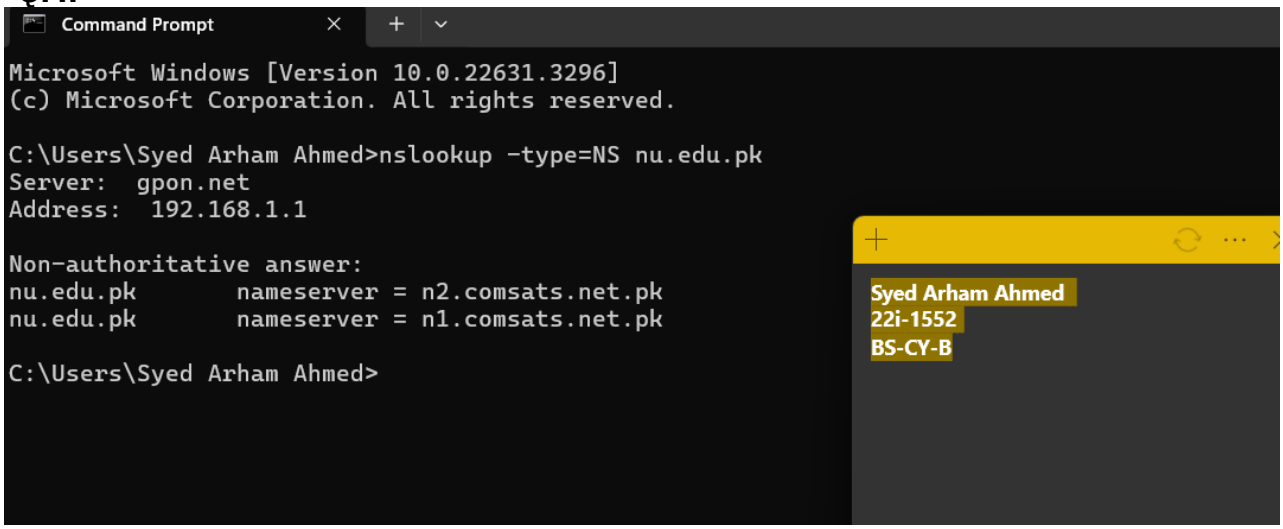
The IP for flex.nu.edu.pk is 115.186.60.84 as shown above.

Q.3.



Its IP address is 192.168.1.1 and its of gpon.net, the command used is nslookup -type=NS nu.edu.pk

Q.4.



The answer came from a non-authoritative server which means it came from a cache of some server rather than an authoritative DNS server.

Q.5.

```
C:\Users\Syed Arham Ahmed>nslookup n1.comsats.net.pk
Server:  gpon.net
Address:  192.168.1.1

Non-authoritative answer:
Name:    n1.comsats.net.pk
Address:  210.56.11.130
```

Syed Arham Ahmed
BS-CY-B
22i-1552

The authoritative server is n1.comsats.net.pk, and its IP is 210.56.11.130, and the command used is nslookup n1.comsats.edu.pk, before this command we used the nslookup -type=NS nu.edu.pk earlier to get to know the name of the authoritative server.

Q.6.

```
C:\Users\Syed Arham Ahmed>nslookup -query=mx nu.edu.pk
Server:  gpon.net
Address:  192.168.1.1

Non-authoritative answer:
nu.edu.pk       MX preference = 10, mail exchanger = aspmx5.googlemail.com
nu.edu.pk       MX preference = 5, mail exchanger = alt2.aspmx.l.google.com
nu.edu.pk       MX preference = 5, mail exchanger = alt1.aspmx.l.google.com
nu.edu.pk       MX preference = 10, mail exchanger = aspmx2.googlemail.com
nu.edu.pk       MX preference = 0, mail exchanger = aspmx.l.google.com
nu.edu.pk       MX preference = 10, mail exchanger = aspmx4.googlemail.com
nu.edu.pk       MX preference = 10, mail exchanger = aspmx3.googlemail.com
```

Syed Arham Ahmed
BS-CY-B
22i-1552

We can see in the screenshot all the mail servers of the NU domain.

Q.7.

```
C:\Users\Syed Arham Ahmed>nslookup -type=NS giki.edu.pk
Server:  gpon.net
Address:  192.168.1.1

Non-authoritative answer:
giki.edu.pk     nameserver = ns2.giki.edu.pk
giki.edu.pk     nameserver = ns.giki.edu.pk
giki.edu.pk     nameserver = localns2.giki.edu.pk
giki.edu.pk     nameserver = localns1.giki.edu.pk
giki.edu.pk     nameserver = ns1.giki.edu.pk
```

Syed Arham Ahmed
BS-CY-B
22i-1552

```
C:\Users\Syed Arham Ahmed>nslookup -type=soa giki.edu.pk
Server:  gpon.net
Address:  192.168.1.1

Non-authoritative answer:
giki.edu.pk
        primary name server = ns.giki.edu.pk
        responsible mail addr = shakir.giki.edu.pk
        serial  = 958
        refresh = 900 (15 mins)
        retry   = 600 (10 mins)
        expire  = 86400 (1 day)
        default TTL = 3600 (1 hour)
```

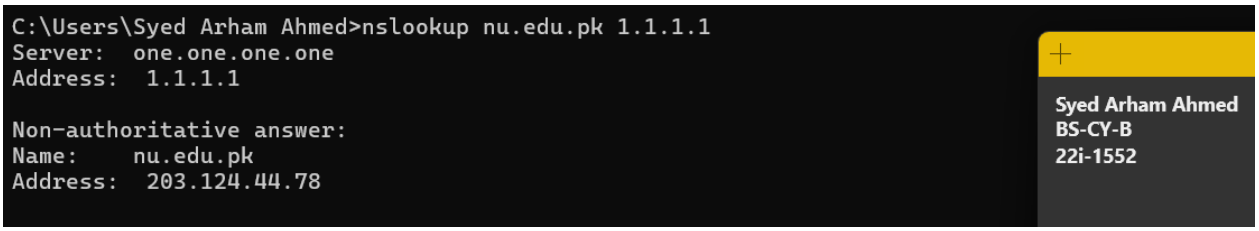
Syed Arham Ahmed
BS-CY-B
22i-1552

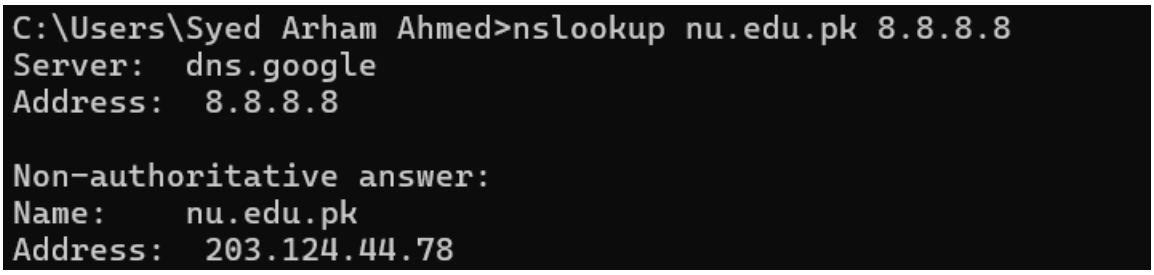
```
C:\Users\Syed Arham Ahmed>nslookup ns2.giki.edu.pk
Server:  gpon.net
Address:  192.168.1.1

Non-authoritative answer:
Name:    ns2.giki.edu.pk
Address:  119.159.235.50
```

Syed Arham Ahmed
BS-CY-B
22i-1552

The first authoritative server returned by nslookup is ns2.giki.edu.pk and to find its IP address we will run nslookup ns2.giki.edu.pk, by this we will get the corresponding IP address of the server.

Q.8.

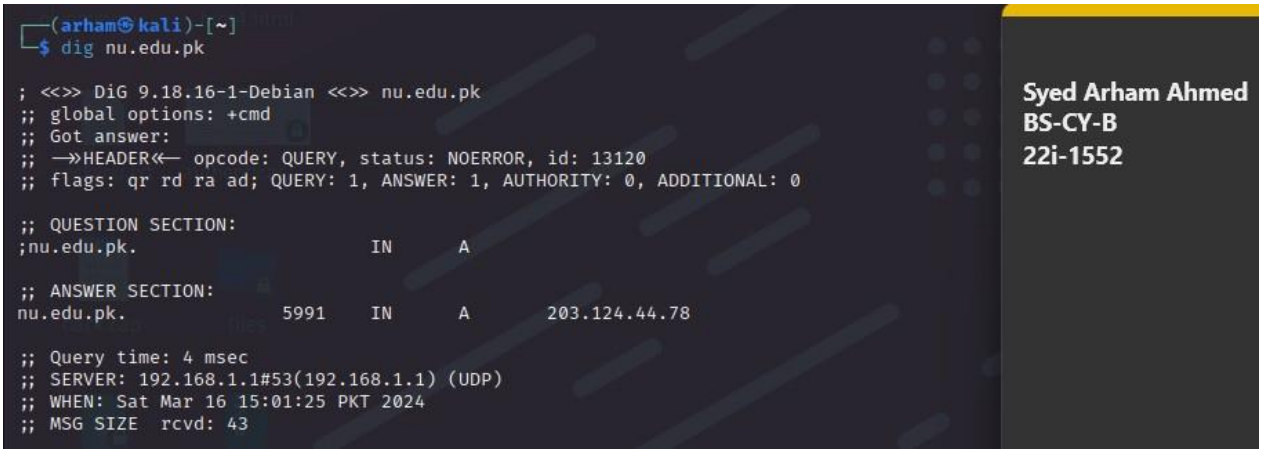




Used Cloudflare and google.

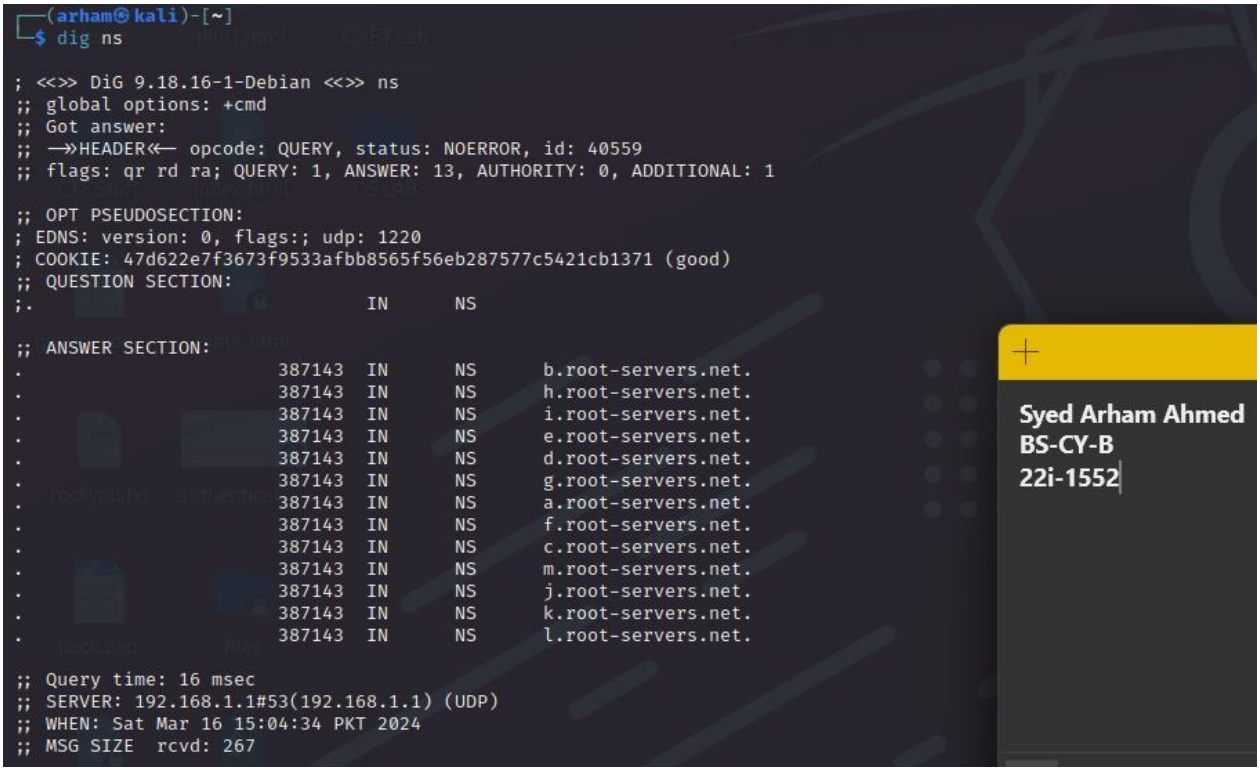
Task#2:

Q.1.



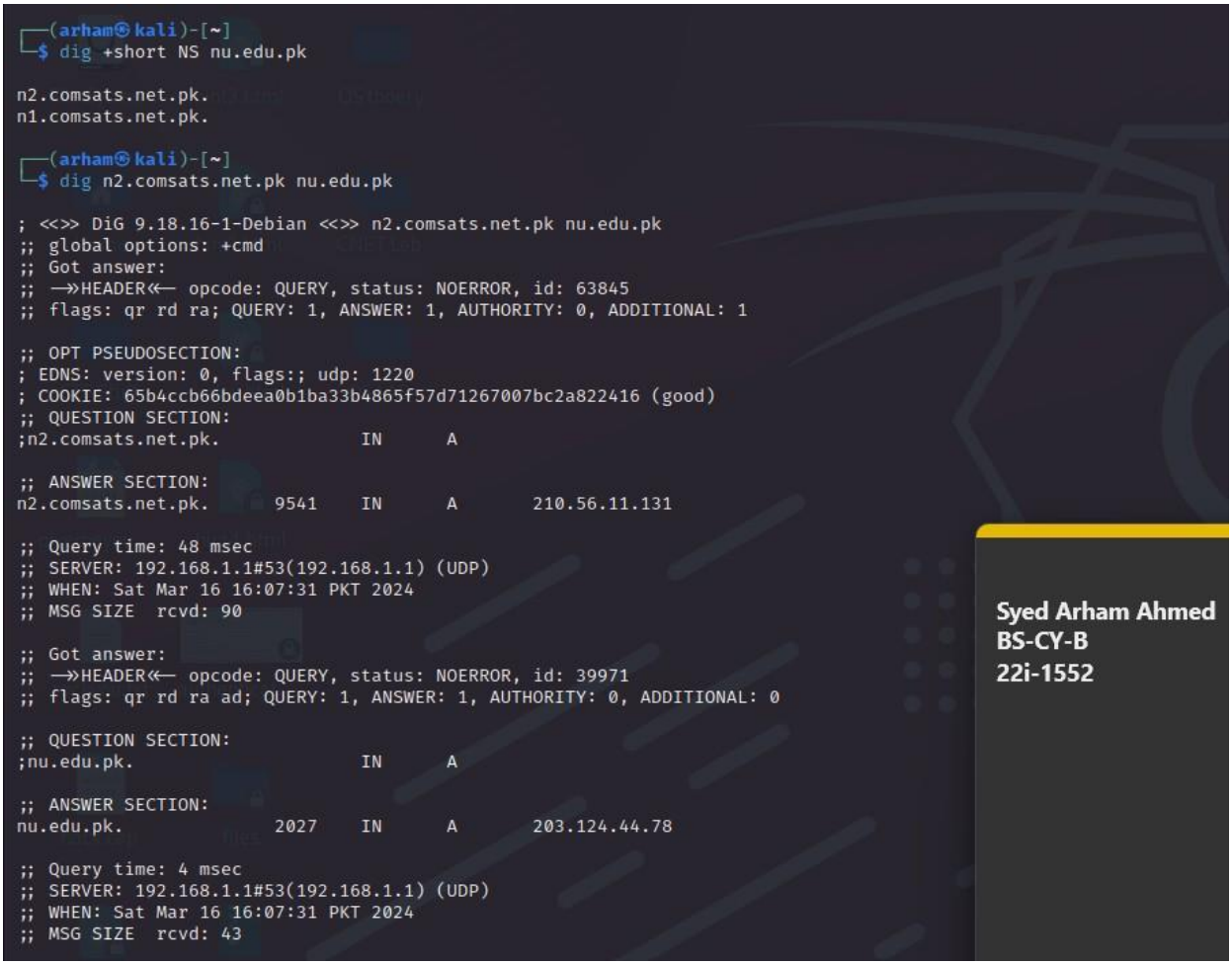
The record type is A, which stands for Address Record.

Q.2.



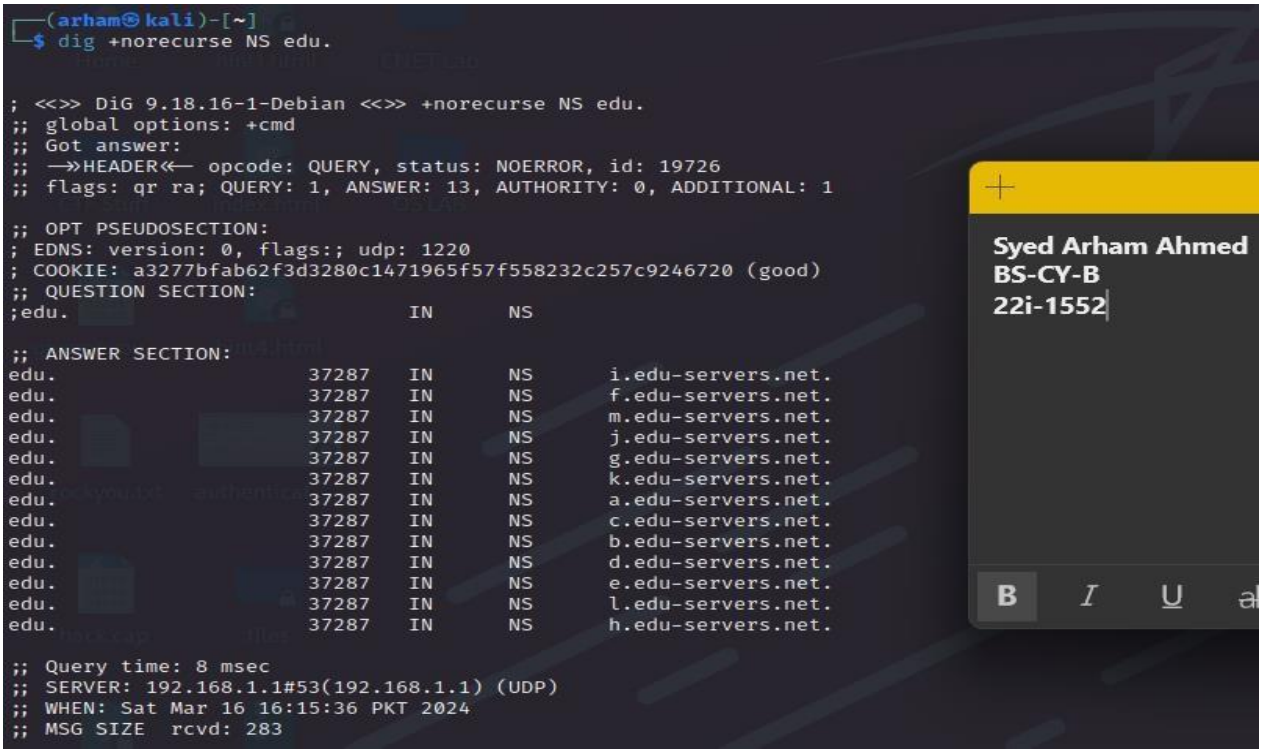
We can see 13 root servers after command dig ns.

Q.3.

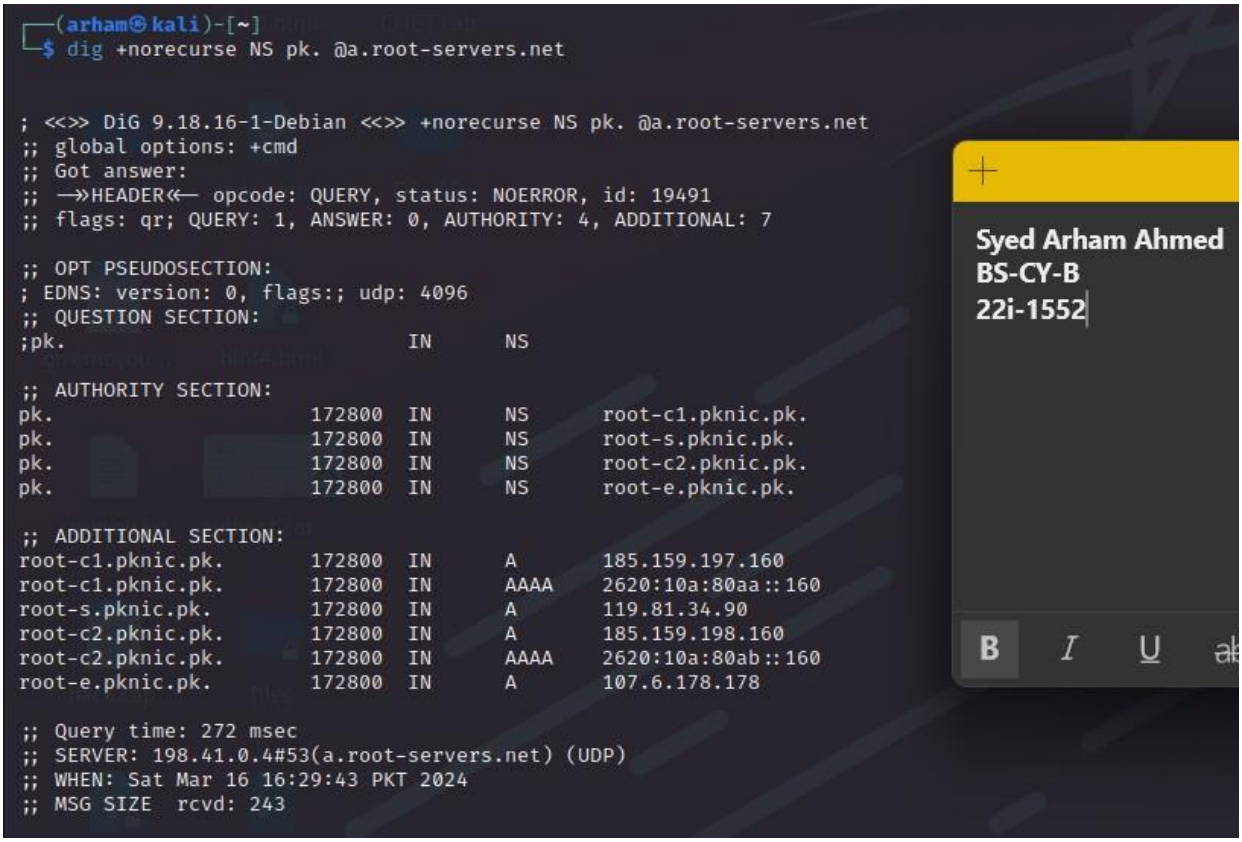


+short just gives the servers then we use dig along with server name to get full information about the server.

Q.4.

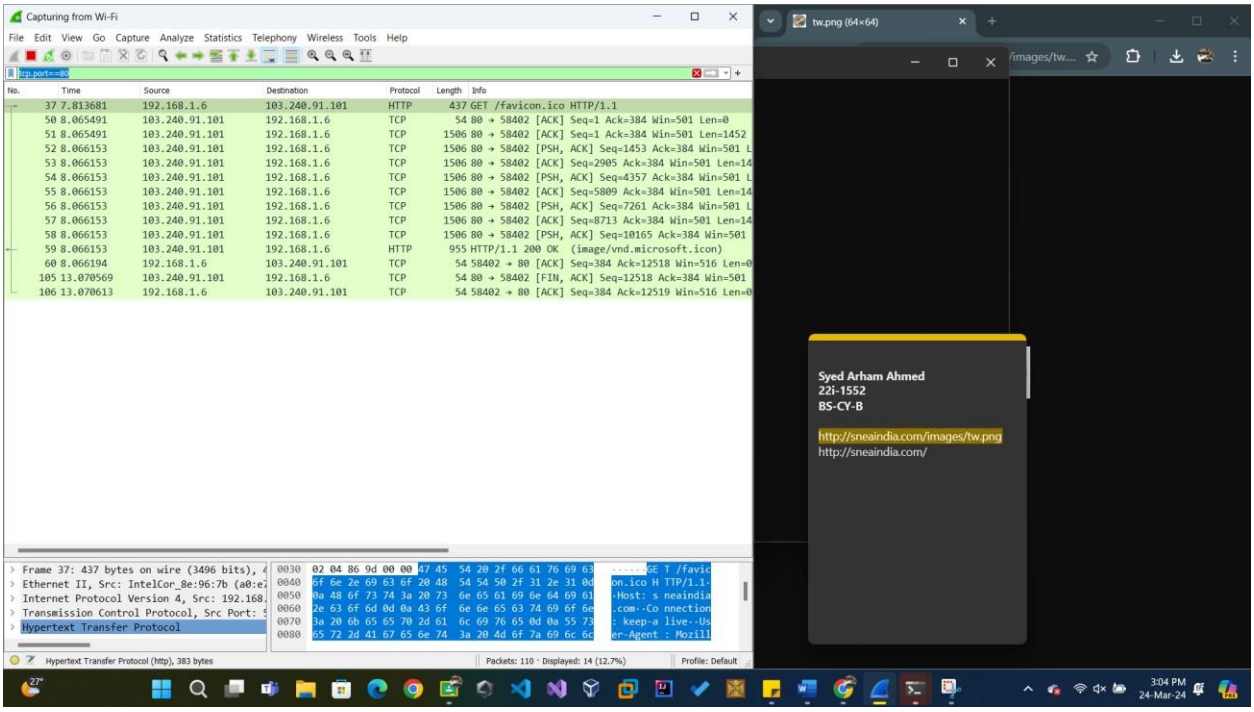

(arham㉿kali)-[~]
$ dig +norecurse NS edu.
; <<>> DiG 9.18.16-1-Debian <<>> +norecurse NS edu.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19726
;; flags: qr ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1220
; COOKIE: a3277bfab62f3d3280c1471965f57f558232c257c9246720 (good)
;; QUESTION SECTION:
;edu. IN NS
;; ANSWER SECTION:
edu. 37287 IN NS i.edu-servers.net.
edu. 37287 IN NS f.edu-servers.net.
edu. 37287 IN NS m.edu-servers.net.
edu. 37287 IN NS j.edu-servers.net.
edu. 37287 IN NS g.edu-servers.net.
edu. 37287 IN NS k.edu-servers.net.
edu. 37287 IN NS a.edu-servers.net.
edu. 37287 IN NS c.edu-servers.net.
edu. 37287 IN NS b.edu-servers.net.
edu. 37287 IN NS d.edu-servers.net.
edu. 37287 IN NS e.edu-servers.net.
edu. 37287 IN NS l.edu-servers.net.
edu. 37287 IN NS h.edu-servers.net.
;; Query time: 8 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Sat Mar 16 16:15:36 PKT 2024
;; MSG SIZE rcvd: 283
Syed Arham Ahmed
BS-CY-B
22i-1552
B I U

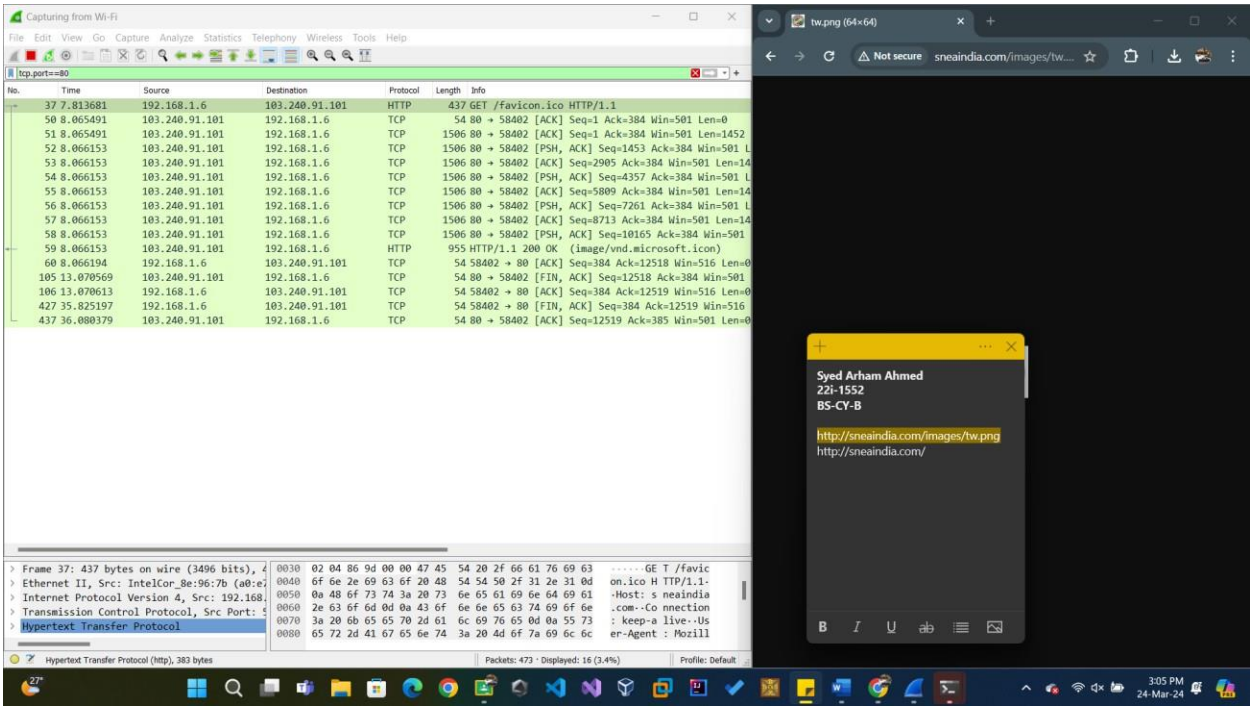
Q.5.


(arham㉿kali)-[~]
$ dig +norecurse NS pk. @a.root-servers.net
; <<>> DiG 9.18.16-1-Debian <<>> +norecurse NS pk. @a.root-servers.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19491
;; flags: qr; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 7
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;pk. IN NS
;; AUTHORITY SECTION:
pk. 172800 IN NS root-c1.pknic.pk.
pk. 172800 IN NS root-s.pknic.pk.
pk. 172800 IN NS root-c2.pknic.pk.
pk. 172800 IN NS root-e.pknic.pk.
;; ADDITIONAL SECTION:
root-c1.pknic.pk. 172800 IN A 185.159.197.160
root-c1.pknic.pk. 172800 IN AAAA 2620:10a:80aa::160
root-s.pknic.pk. 172800 IN A 119.81.34.90
root-c2.pknic.pk. 172800 IN A 185.159.198.160
root-c2.pknic.pk. 172800 IN AAAA 2620:10a:80ab::160
root-e.pknic.pk. 172800 IN A 107.6.178.178
;; Query time: 272 msec
;; SERVER: 198.41.0.4#53(a.root-servers.net) (UDP)
;; WHEN: Sat Mar 16 16:29:43 PKT 2024
;; MSG SIZE rcvd: 243
Syed Arham Ahmed
BS-CY-B
22i-1552
B I U

Task#3:

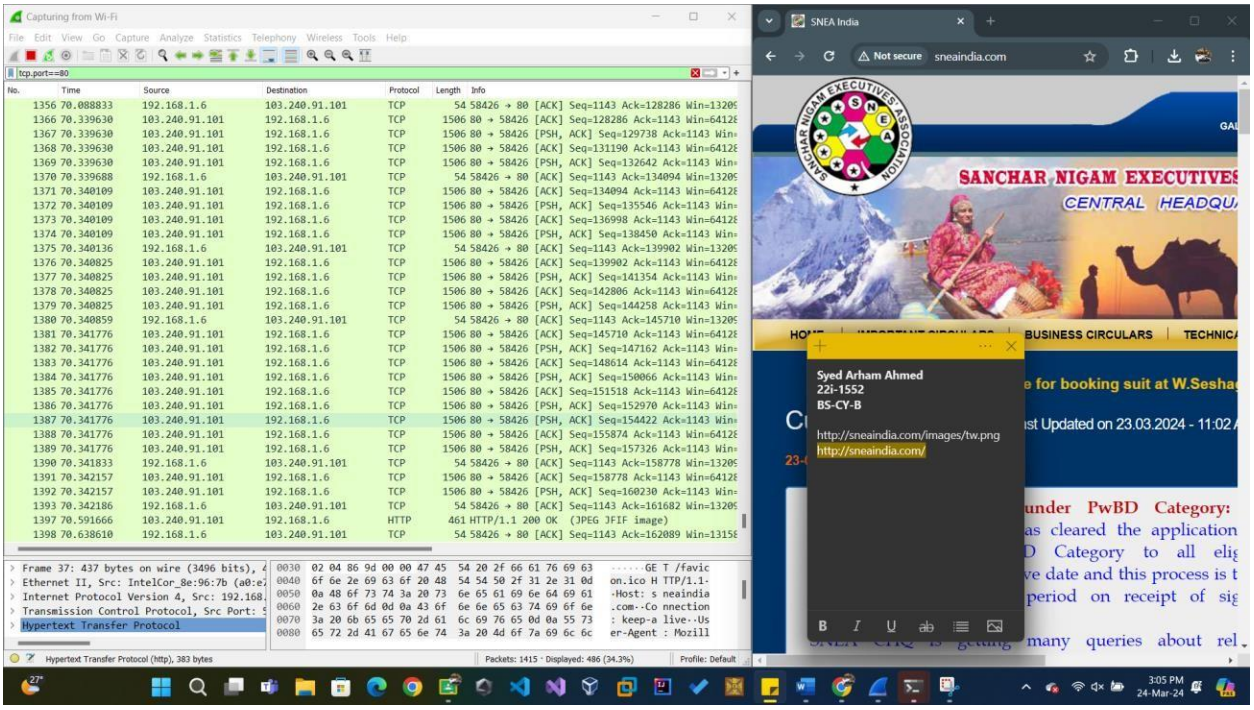
Q.1.





So, the difference that I noticed now is that when I re-pasted the URL is that it did not generate more than 2 more packets, this means that cache was used to fetch the URL contents, and it did

not do TCP handshake again as well saving us time when re opening the URL. I can also see the HTML code of the still webpage if I follow and open HTTP stream of the packets.



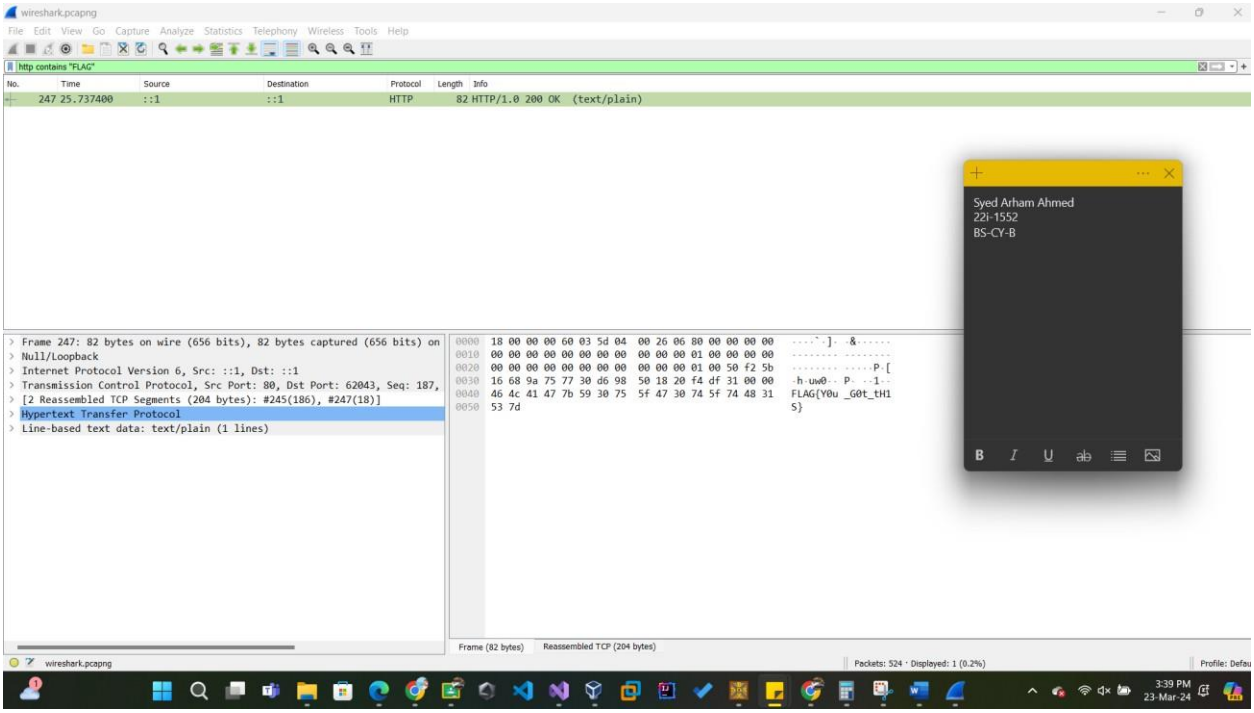
Well, the static image URL did not generate many packets but the whole website generated thousands of packets as a lot more data needed to be loaded other than just still images with no embeds.

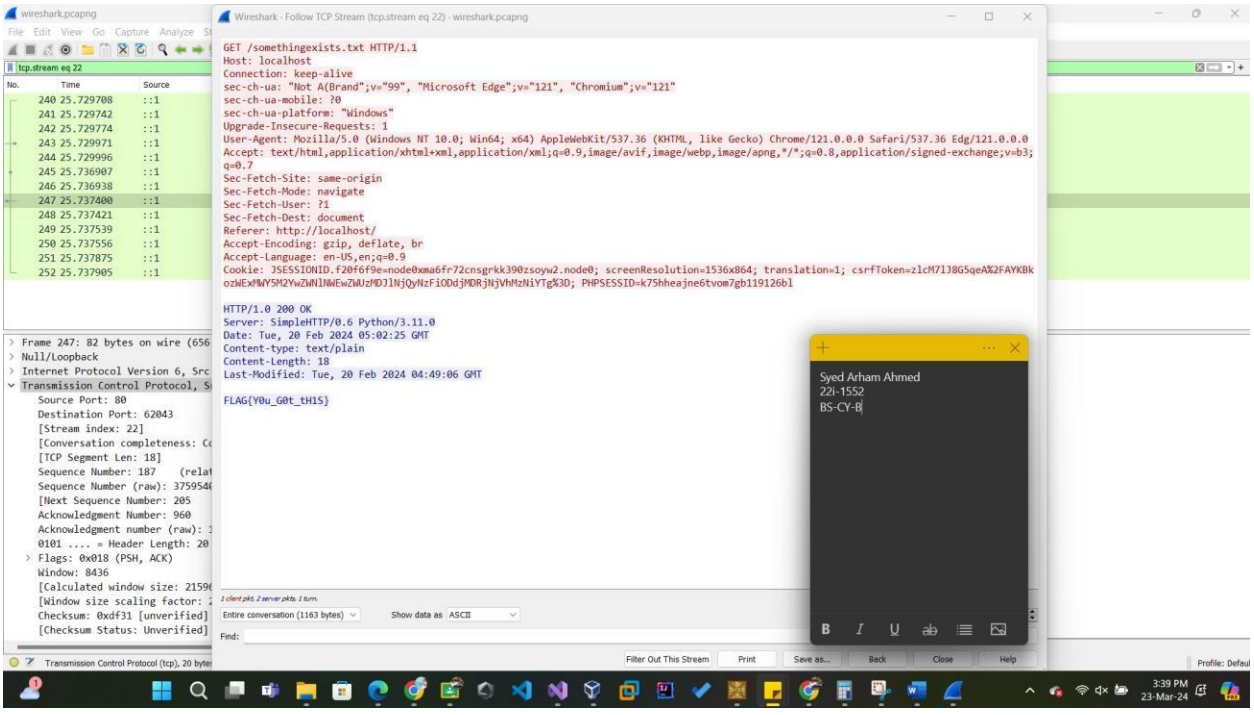
Syed Arham Ahmed_22i-1552_BS-CY-B_CNET_Assignment#2

Q.2.

http contains "FLAG" {This command searches for the word FLAG in the TCP packets}

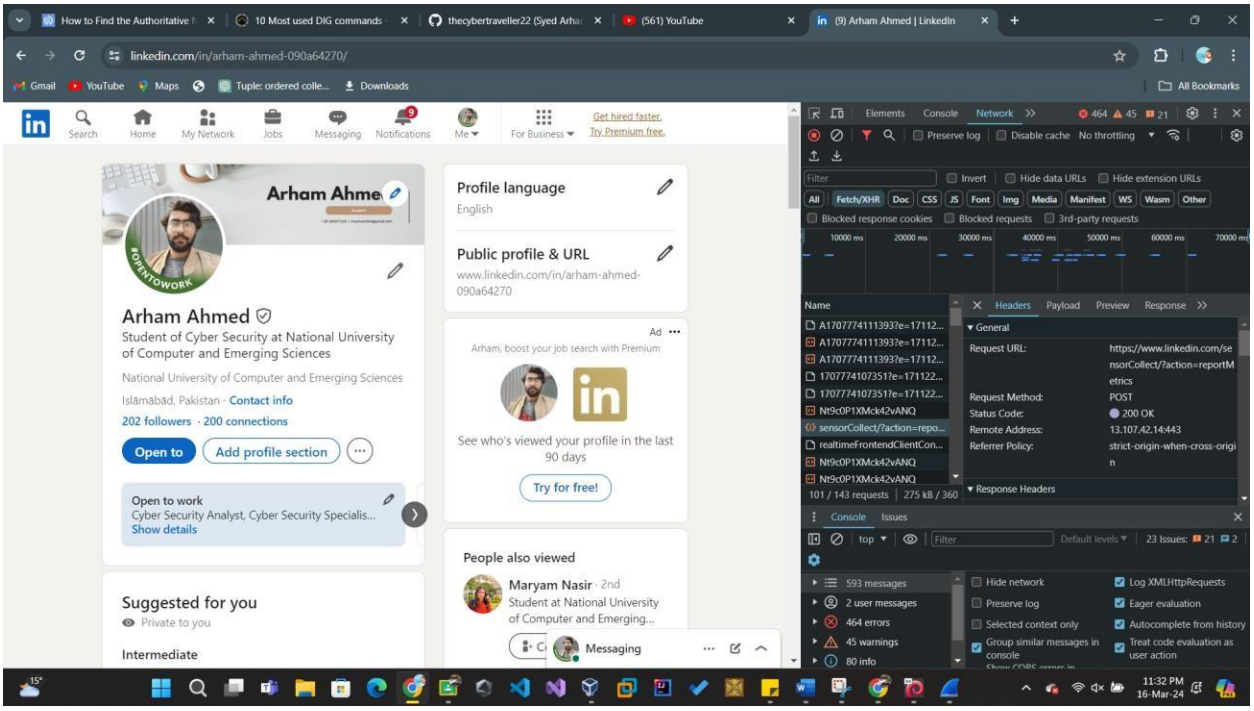
I ran the command listed above and it gave me the packet ie:247 which contains the flag.



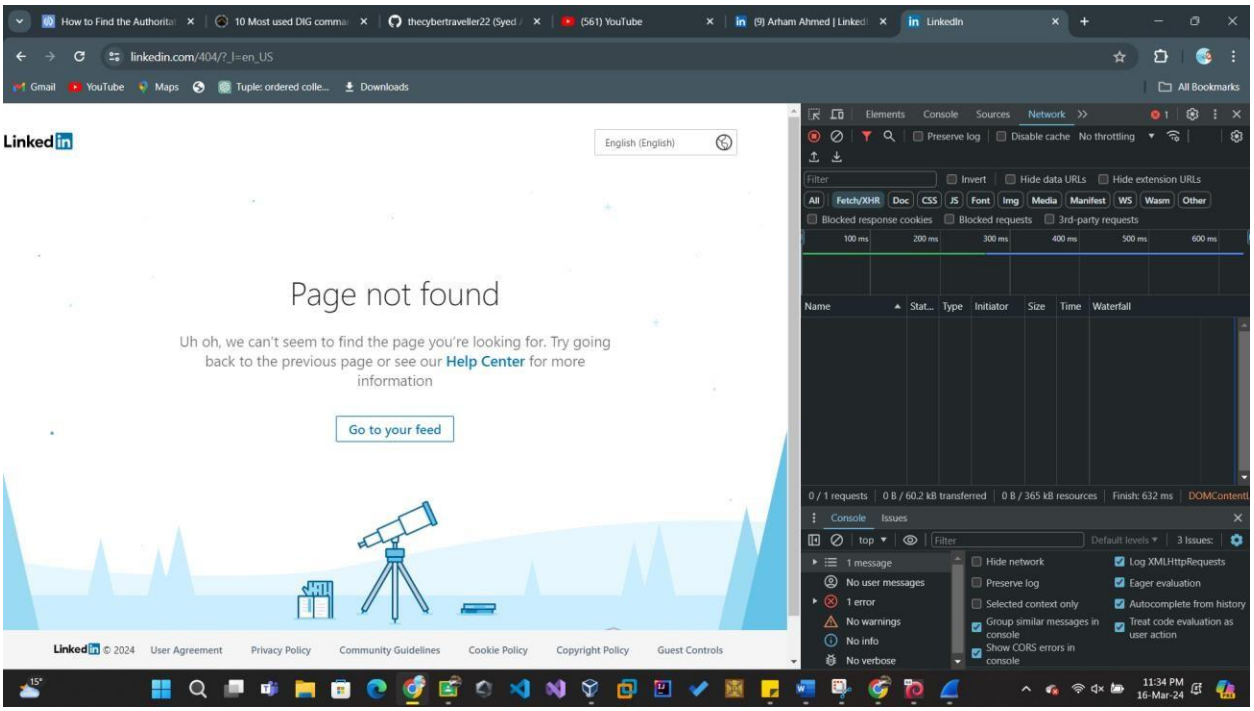


Syed Arham Ahmed_22i-1552_BS-CY-B_CNET_Assignment#2

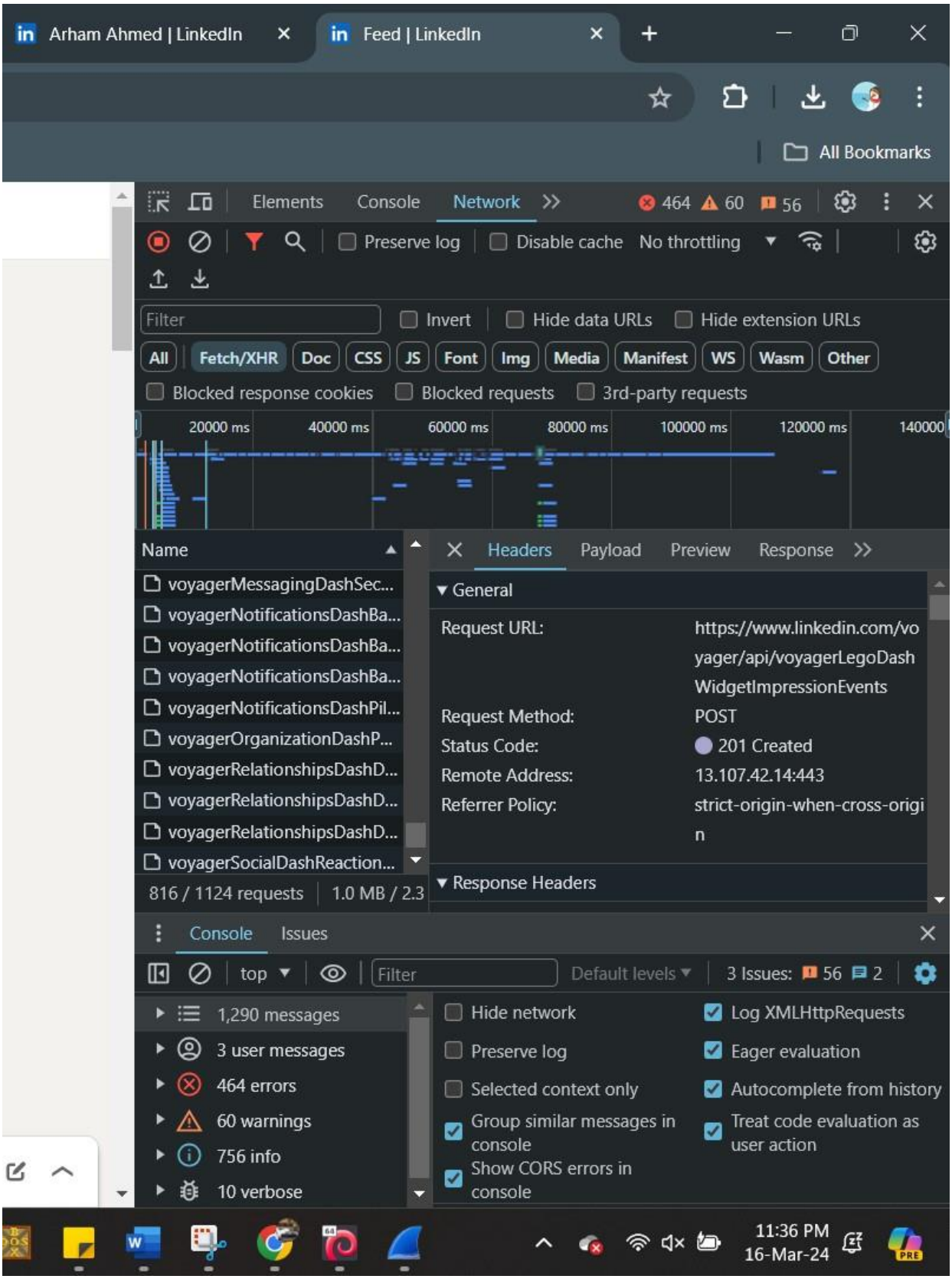
Q.3.



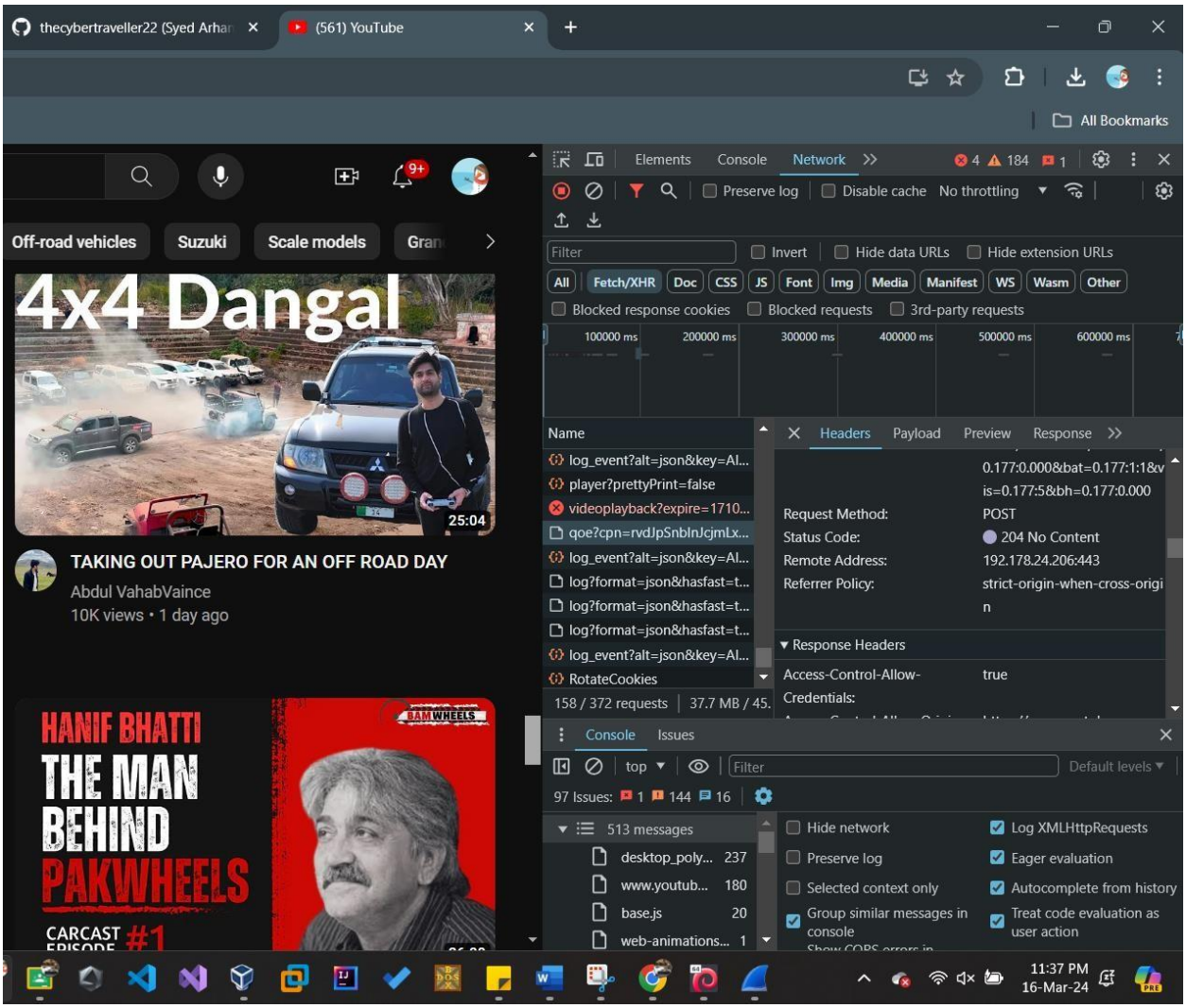
Syed Arham Ahmed_22i-1552_BS-CY-B_CNET_Assignment#2



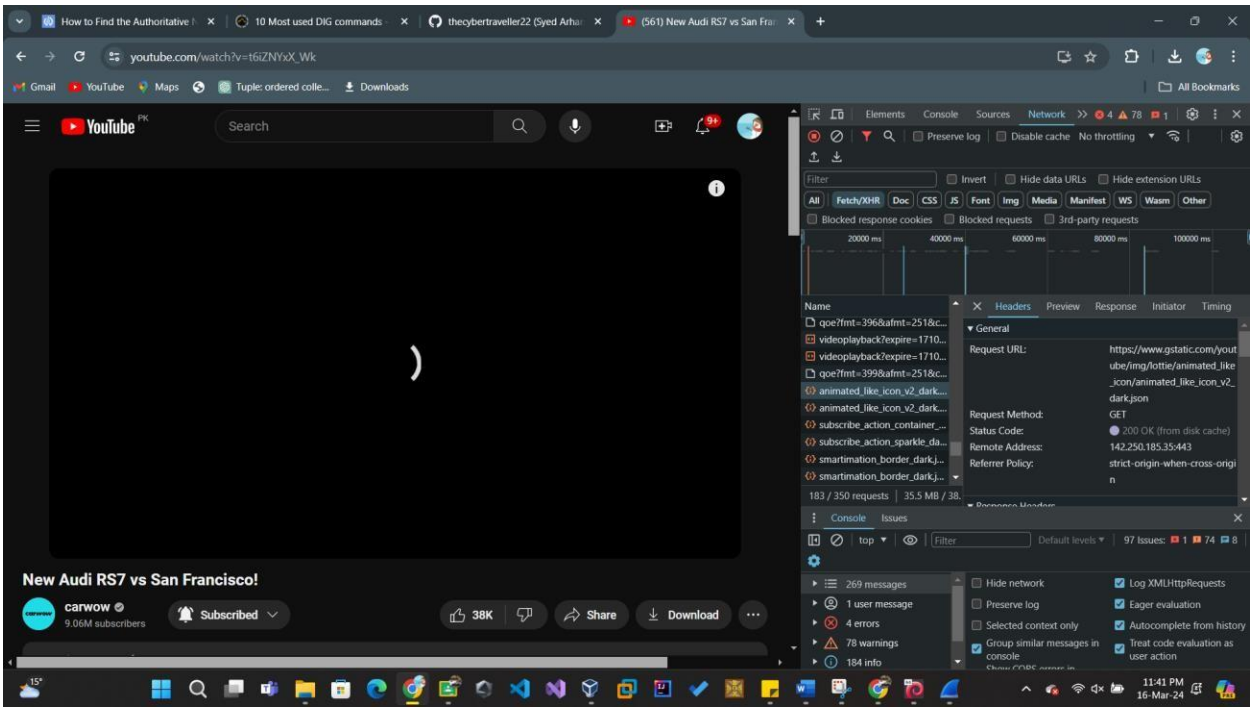
Syed Arham Ahmed_22i-1552_BS-CY-B_CNET_Assignment#2



Syed Arham Ahmed_22i-1552_BS-CY-B_CNET_Assignment#2



Syed Arham Ahmed_22i-1552_BS-CY-B_CNET_Assignment#2



The above image shows us that it got the data from the cache instead of asking the DNS server.